DEPARTMENT OF THE ARMY
HEADQUARTERS AND HEADQUARTERS COMPANY, 22D SIGNAL BRIGADE
UNIT 29500
APO AE 09175-9500

AETV-SBH-CO

12 July 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Letter 4, Information Assurance

1. References:

a. AR 385-19, Information Systems Security, 27 February 1998.

b. Army in Europe Command Policy Letter 4, Information Assurance, 4 May 2003.

2. As we continually transform our information systems into a global information network, seamless across platforms and interfaces, our vulnerability significantly increases. Our best defense against this vulnerability is our absolute commitment to information assurance.

3. As the communications element for V Corps, it is our responsibility to protect our automated information systems, preserve the integrity in the information and the data used by the combatant commanders to affect the battle and win the war. To this end, it is our duty to ensure that every user of a computer system must know how to protect, recognize, and respond to attacks on our information systems.

4. Every information technology professional will complete the USAREUR Information Assurance/Computer network Defense Training program before assuming duties directly interfacing network systems.

5. Every individual must be aware of the policies and procedures governing information systems and computers. Each individual will successfully complete the USAREUR Computer User Test before being given access to any system. Documentation will be maintained in the Brigade Automation section and inspected randomly to ensure compliance.

6. Every information system employed must comply with published standards, baselines, and information assurance vulnerability alerts (IAVAs) as directed by the USAREUR Information Assurance Program Manager.

7. The Information Assurance Officer will conduct quarterly training on information assurance programs. Records of this training will be maintained on file and anyone not

completing this training will have their user rights suspended until their training is complete.

8. Computer users will maintain responsibility for their data and must be aware of the dangers of transferring data to/from home and office information systems. This includes the use of removable devices and media. Government computers are provided to the individual specifically for government business. Computer systems are monitored at all times and users violating computer use policy will be considered for UCMJ action.

9. EAGER ELITES!

Charles D Smith
CHARLES D. SMITH
CPT, SC
Commanding

Distribution:
A